オーバーレイネットワーク用端末識別子共有を目指した認証連携機能の研究

B23722 宮村一希 指導教員 内藤克浩

キーワード: Sigle Sign-On, OpenID Connect, Linkage service, Overlay Networks, End-to-end communication

1 はじめに

近年, 端末間の直接通信を実現する E2E は, ネットワーク負荷や通信遅延低減の観点からビデオ会議やオンラインゲーム等のサービス開発者に注目されている. しかし, 現在の E2E はファイヤウォールルータの機能（NAPT）と IPv4 と IPv6 間の非互換性による通信阻害やネットワーク移動時の通信切断の問題が存在する. 本研究室ではサービスに E2E 通信を提供するために, CYber PHysical Overlay Network over Internet Communication（CYPHONIC）と呼ばれるオーバーレイネットワークプロトコルを提案している [1]. CYPHONIC を使用するサービスは CYPHONIC Fully Qualified Domain Name（FQDN）と呼ばれる識別子の使用を前提としている. しかし, 現在の CYPHONIC では, この CYPHONIC FQDN をサービスが認知する手段が確立されていない.

この CYPHONIC FQDN は, CYPHONIC のユーザアカウント情報に紐づいている. したがって, 本研究ではサービスが CYPHONIC のアカウント情報を用いて認証を行い, 認証後に CYPHONIC FQDN を提供する機能を提案する. CYPHONIC FQDN 提供の際, 認証を行うことにより, 第三者に CYPHONIC の情報が漏洩することを防ぐことが可能である. 加えて, サービスが CYPHONIC のアカウントによる Single Sign-On（SSO）が可能となる. 本研究を実現するため, OpenID Connect（OIDC）の仕様に則り CYPHONIC の拡張を行う [2]. その後, 本研究の性能評価と拡張による CYPHONIC への影響を評価する.

2 CYPHONIC

CYPHONIC は, CYPHONIC を使用して通信するデバイスである CYPHONIC ノードと, これらのノードによる通信を管理する CYPHONIC クラウドで構成される. CYPHONIC クラウドは, デバイス認証を行う Authentication Service（AS）と, デバイスのネットワーク情報を管理する Node Management Service（NMS）, デバイスと直接通信不可能な場合に中継を行う Tunnel Relay Service（TRS）で構成されている.

CYPHONIC クラウドは, CYPHONIC ノードに仮想 IP アドレスとそれに紐づいた CYPHONIC FQDN を提供することで, 仮想 IP アドレスで通信を行うオーバーレイネットワークを構築する. サービスは, CYPHONIC FQDN をソケットの宛先として使用すると, 端末に常駐するアプリケーションがパケットを拾い上げて CYPHONIC クラウドに経路構築を指示する. この仕様により, サービス開発者はリアルタイムゲームやビデオ会議等の E2E サービスを容易に作成可能である.

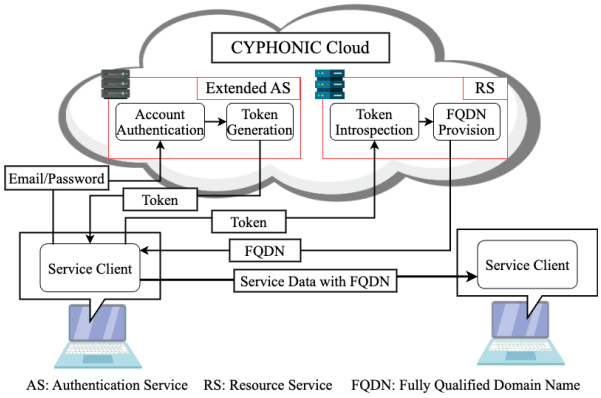

図 1: 提案機能の概要

3 提案システム

CYPHONIC FQDN は相手端末との通信を行うために必要である. したがって, サービスは CYPHONIC FQDN を認知する必要がある. しかし, CYPHONIC クラウドには機密性の高いユーザ情報が含まれているため, 限られた情報をサービスと安全に共有するための設計が必要となる.

本研究では, OIDC を利用して CYPHONIC 情報と連携認証をサービスにセキュアに提供する SSO 機能を提案する. 図 1 に提案機能の概要図を示す. SSO を実現するため, OpenID Provider（OP）機能を AS の拡張として CYPHONIC クラウドに追加した. この機能は認証と CYPHONIC 情報取得用トークンの管理を行う. サービスが本機能を使用する際, AS に認証リクエストを送信する. 認証の際, サービスの利用者は CYPHONIC アカウントに紐づく Email アドレスとパスワードを送信する. 認証後, AS は CYPHONIC FQDN へのアクセスを許可するトークンを発行する. その後, ユーザはサービスのページにリダイレクトされ, 認証を完了する.

また, CYPHONIC のアカウント情報を提供する Resouce Service（RS）機能を追加した. RS はサー

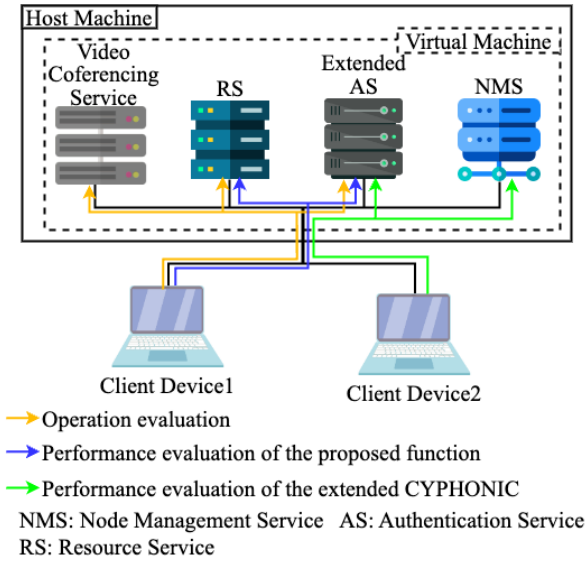

図 2: 検証の概要

ビスによって送信されたトークンの検証を行う．検証後, RS はトークンに紐づいた自身の CYPHONIC FQDN をサービスに送信する．

4 検証及び評価

本検証では, 提案する認証連携機能を搭載した CYPHONIC オーバーレイネットワーク上で動作するビデオ会議ツールを開発し, 実証を行った．このビデオ会議サービスは, CYPHONIC アカウントによる連携認証後に自身の CYPHONIC FQDN を取得して通話相手と交換をすることにより, 通信相手の通信識別子を認知している．検証の概要図を図 2 に示す．本実証では, CYPHONIC クラウドとビデオ会議サービス用クラウドを含むクラウドサービスと二台のユーザデバイスを用意した．クラウドサービスは, Intel Core i9-11900K @ 3.50GHz の CPU と 128GB のメモリを搭載したホストマシン上で動作する, メモリ 4GB の仮想サーバを用意した．ユーザマシンは, Intel Core i5-1135G7 @ 2.40GHz の CPU と 8GB のメモリを搭載したラップトップ PC を用意した．

はじめに, ビデオ会議ツールを使用し, 実際に認証連携機能が動作するか実証を行った．本動作検証では, CYPHONIC のアカウントに Email とパスワードでログインし, アカウントに紐づいた CYPHONIC FQDN を取得し CYPHONIC オーバーレイネットワーク上でビデオ会議が可能か確認した．検証の結果, CYPHONIC アカウントへのログイン, CYPHONIC FQDN の取得, オーバーレイネットワーク上でのビデオ会議の動作を確認した．

次に, 提案機能自身の性能を評価するため, 提案機能のシグナリングに要する時間を測定した．測定するシグナリングは, 認証, トークンの発行, FQDN の取得の 4 種類である．各シグナリング毎に 100 回づつ計測を行った．表 1 にシグナリング所要時間の計測結果を示す．計測結果から, 本機能のシグナリング所要時間は許容範囲内に収まっていることが分かる．

表 1: 提案機能のシグナリング所要時間

処理名	通信所要時間
認証	32 ms
トークンの発行	90 ms
FQDN の取得	53 ms

表 2: CYPHONIC のシグナリング所要時間

処理名	既存 CYPHONIC	拡張 CYPHONIC
ログイン	29.54 ms	34.37 ms
経路構築	41.37 ms	48.45 ms

最後に, SSO 機能がどれほどクラウドサービスの処理負荷を増加させるか検証するため, CYPHONIC のシグナリングオーバーヘッドを計測した．本計測では認証のためのログイン処理と通信開始のための経路構築処理に着目した．表 2 に CYPHONIC クラウドのシグナリング時間の比較を示す．その結果, 性能劣化は許容範囲内に収まっていることが分かる．

5 まとめ

本研究では, サービスに CYPHONIC の情報と連携認証を安全に提供する, CYPHONIC の SSO 機能を提案した．評価結果より, 本機能によりサービスが CYPHONIC 上の端末識別子を取得し, 相手端末と通信可能であることを実証した．また, 提案機能の性能および, 拡張を施した CYPHONIC クラウドの性能変化が許容可能な水準であることを確認した．

研究業績

- K. Miyamura, et al.: “Single Sign-On function of CYPHONIC for service linkage,” *2024 IEEE 13th Global Conference on Consumer Electronics (GCCE)*, October 2024.

参考文献

[1] T. Yoshikawa, H. Komura, C. Nishiwaki, R. Goto, K. Matama, and K. Naito, “Evaluation of new CYPHONIC: Overlay network protocol based on Go language,” in *2022 IEEE International Conference on Consumer Electronics (ICCE)*, pp. 1–6, January 2022.

[2] W. Li and C. J. Mitchell, “Analysing the security of google’s implementation of openid connect,” in *Proceedings of the 13th International Conference on Detection of Intrusions and Malware, and Vulnerability Assessment - Volume 9721*, p. 357–376, June 2016.